Genetec ClearID™

Unified physical identity and access management

Genetec™

A smarter way to manage access

The seamless movement of people through an organization is integral to its success. How you assign and manage access rights helps to protect that flow. But over time, compliance needs, new processes, and external regulations can slow things down – introducing gaps in security and interrupting that all-important momentum.

Often, it's little things like lost cards and access requests that take up an operator's valuable time. And because typical access control systems are static and unlinked to company policies, the operator has no clear administrative path to follow.

Genetec ClearID™ offers a more intelligent solution. It's a self-service physical identity and access management system that enforces your security policies, helping to make your organization more efficient, compliant, and secure. It can be deployed faster and with greater ease than other integrated systems because it's unified with our access control security software, Security Center Synergis™. And because ClearID is a cloud-based service, it works natively with Synergis – which means goodbye to endless customizations and clunky component integrations.

From corporate offices and university campuses to highly regulated multinationals in the oil, gas, mining, and petrochemical industries, ClearID delivers a smooth transition away from the day-to-day complexities of managing individual access rights.

Guided by your policies, ClearID's automated and self-service capabilities enable a more fluid, efficient working environment for everyone.

Identities explained

ClearID centrally manages the access rights of all the individuals who interact with your organization. Here's what you need to know:

Identity

An identity is an employee's or visitor's unique digital profile. It can be permanent for employees, semi-permanent or temporary for visitors. Identities interact across many security and business systems and might comprise:

— An employee in the payroll and human resources management system
— A Windows user in Microsoft Active Directory
— A sales manager in the customer relationship management and quoting tool
— A cardholder in the physical access control system

Identity lifecycle

From admitting visitors to onboarding and offboarding employees, a modern physical identity and access management solution (PIAM) centrally manages an organization's policies, processes, and identities. Once policies are defined, ClearID will oversee the lifecycle of an identity across four typical stages:

1. Identity creation
2. Access provisioning
3. Identity evolution
4. Access termination

Attributes

An identity is composed of a set of characteristics called attributes. These attributes are used to define an identity's access rights. As someone's attributes evolve, so do their access rights.

Examples are:
— Department
— Location
— Role
— Name of supervisor
— Title of employee
— Seniority
— Training

How ClearID works

ClearID empowers organizations to standardize and enforce their security and compliance policies. By automating and simplifying access rights management, the security and operational risks are mitigated. It's a streamlined workflow that covers these steps:

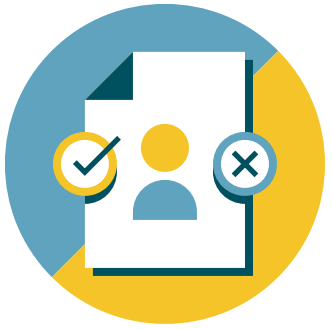
Step 1: Initial request

An employee connects to ClearID and requests access to a secure area for a specific duration.

Step 2: Verification and supervisor approval

When an access request is made, ClearID verifies the policies for the location and auto-approves or seeks approval from authorized supervisors.

Step 3: Access rights modification



If approved, the access control system is updated, granting the right access for the time period requested. If declined, access is denied, and the applicant receives an email explaining why.

Smoothing out cardholder experience

Every day, your employees and visitors rely on the physical access control system to navigate across your facility, from common areas to more secure locations. So why limit the ability to modify access rights to security operators or IT staff? In most cases, when someone needs to request a change, they have to visit the badge office or receptionist, further delaying the process.

As a self-service physical identity and access management solution, ClearID gives everyone a new, workflow-based approach to request new access privileges or change existing ones. Requests can be made directly with area owners without involving access control system operators.

By giving employees and visitors control over their access requests, ClearID improves the cardholder's experience, reduces frustrating delays, and keeps your organization moving.

Heightening security, lowering risk

Offboarding is a crucial moment in the employee exit process. After all, when an employee is offboarded, they should no longer have access to your facilities and especially secure areas. But sometimes an operator might not know the right policies to follow to terminate access or might not be aware of all the workarounds and exceptions programmed into an access control system.

Small improvisations are generally made by individual operators and are not always centrally controlled. Over time, these policy workarounds accumulate, creating security gaps.

With ClearID, you define your standard security and compliance policies and it takes care of the rest. Its workflow engine relies on organizational policies to continuously update individual access rights based on current identity attributes. The slightest change to an attribute modifies existing access rights, eliminating the need for manual exceptions or ad hoc modifications.

So, when your HR team deactivates an employee's identity, their access is revoked in all systems, ensuring proper offboarding.

Enhancing methodical oversight

In their day-to-day job, operators sometimes make exceptions to their organization's corporate policies. For example, an operator might receive a call from an employee's supervisor and grant access on an exceptional basis.

In a traditional system, the change is implemented but, more often than not, the approval and the reason for it are never captured.

ClearID tracks and reports every operation or action tied to an identity throughout their lifecycle. From temporary or permanent access requests and approvals, it paints the full picture by providing the context behind exceptions and one-time requests. This helps organizations perform routine access reviews and audits to validate that all employees and visitors only have access to authorized areas.

Making your organizational security fully traceable allows you to safeguard compliance with regulations and corporate governance.

Improving operational efficiency

Traditional access control systems rely on operators to issue credentials and authorize access. But how can a small number of personnel be expected to know the access rights of every employee or visitor?

When proof of training is required for specific areas, operators will typically need to contact an area owner or supervisor for confirmation or sift through their emails to find the approval. This manual approach is invariably delayed when supervisors are in a meeting or on vacation. As an organization grows, this method necessitates more operators to deal with greater numbers of cardholders and areas.

Organizations often address the problem of an overloaded or overworked team by hiring more personnel, but this only masks the underlying inefficiency of a manual system. By automating access rights management and reducing bottlenecks, ClearID ensures that employees and visitors have met all corporate requirements before providing access to an area. That means the management of day-to-day access requests, compliance, and policy updates is significantly improved. Operators become more efficient and direct their focus to high-risk, mission-critical work.

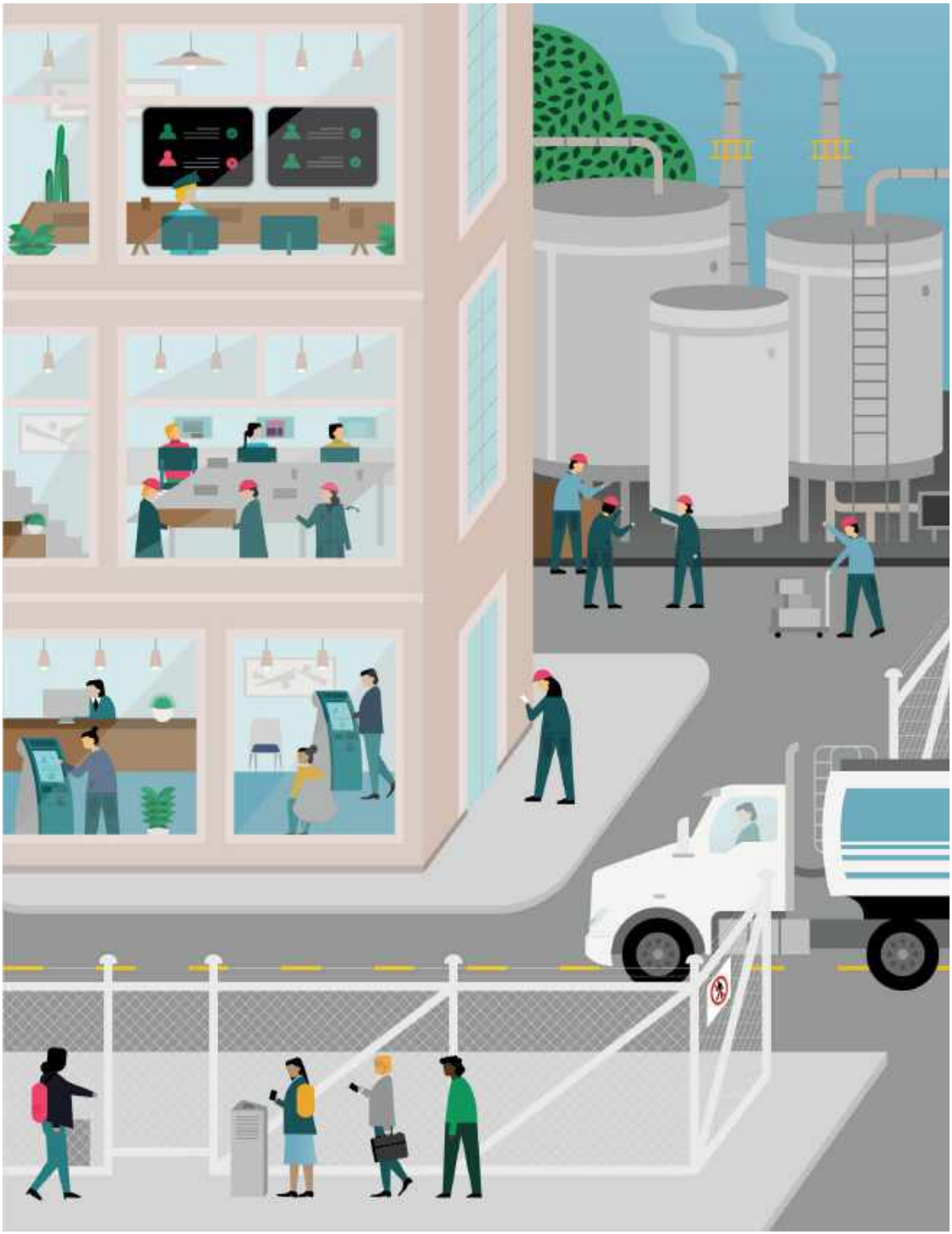
Improve your visitors' experience

In a busy corporate office, admitting visitors can be a labor-intensive task for front-desk staff. Activities range from reading incoming email requests and adding visitors to the daily visitor list to manually checking-in visitors and calling their hosts. Time-consuming and inefficient, this approach leads to longer visitor wait times that may leave your guests with less-than-stellar first impressions.

With ClearID, visitor management becomes a smoother experience for everyone. As soon as a meeting is arranged, the process begins. First, the local employee (or host) logs into ClearID over a web portal and creates a profile for her visitor, providing his name and contact details, as well as the purpose, date, time, and duration of the visit. The meeting request needs to be approved by the host's manager or ClearID can automatically approve the meeting providing the right criteria are met. The visitor then receives an email invitation from ClearID on behalf of the host's organization.

Meanwhile, approval for the visit is automatically granted by ClearID as the host has been permitted by a system administrator to invite a guest without supervisor approval. The visitor and host both receive confirmation emails for the upcoming appointment. On the day of the meeting, the visitor arrives at the front lobby and scans his email QR code or ID at a kiosk.

After sign-in, a visitor sticky badge is printed at the kiosk or an active credential is given by the receptionist – and the host is notified of his arrival. The host now greets her visitor and escorts him to the conference room, where they get to work on time and without complications.



Preparing for an audit

In an industry where organizations need to comply with strict access requirements, regular audits are essential. For example, a supervisor is informed of an upcoming audit and reaches out to the security director so he can get a report on who has access to restricted areas. But the security director is on vacation, which means running the report becomes convoluted and time-consuming. Once it's finally handed over, the supervisor notices how many unauthorized people have had access to these restricted areas. They include former visitors and employees who have left the organization.

If the regulating body were to find out, the organization would be handed a hefty fine for breaching regulations. Now, the supervisor will have to review every person on the report and identify who should continue to have access. Once finalized, he'll need to send a report of people who need to be removed so that the security director can update the access control system. This manual process is painfully slow, resource dependent, and open to human error because someone on the list could easily be missed.

With ClearID, the supervisor can log into the portal to quickly see who has access to rooms and areas and revoke the people who shouldn't be there. He can simply pick the location he wants to verify and then instantly revoke a person's access to that room – with the option to provide a reason. What used to be a costly manual process can now be done in minutes – putting control back in the hands of the supervisor and saving the organization thousands in fines.

Security that keeps you moving

ClearID allows you to standardize and automate your security policies, reducing inconsistencies and eliminating security gaps. In the process, it helps you achieve and maintain compliance with organizational or industry regulations across all your sites. Operationally, you achieve new levels of efficiency by centrally managing identities and by empowering employees through a self-service model for access control. ClearID keeps your organization moving steadily along with confidence.

Corporate Headquarters
Genetec Inc.
2280 Alfred-Nobel Blvd.,
Suite 400
Montréal QC H4S 2A4
Canada
Toll Free: +1 866 684 8006
Canada & USA:
Tel: +1 514 332 4000
genetec.com

Genetec ClearID is a self-service physical identity and access management system that standardizes and enforces your security policies to authorize access and make your organization more efficient.

genetec.com/clearid